Procedure om de AMP-connector te verwijderen als het wachtwoord wordt vergeten

Inhoud

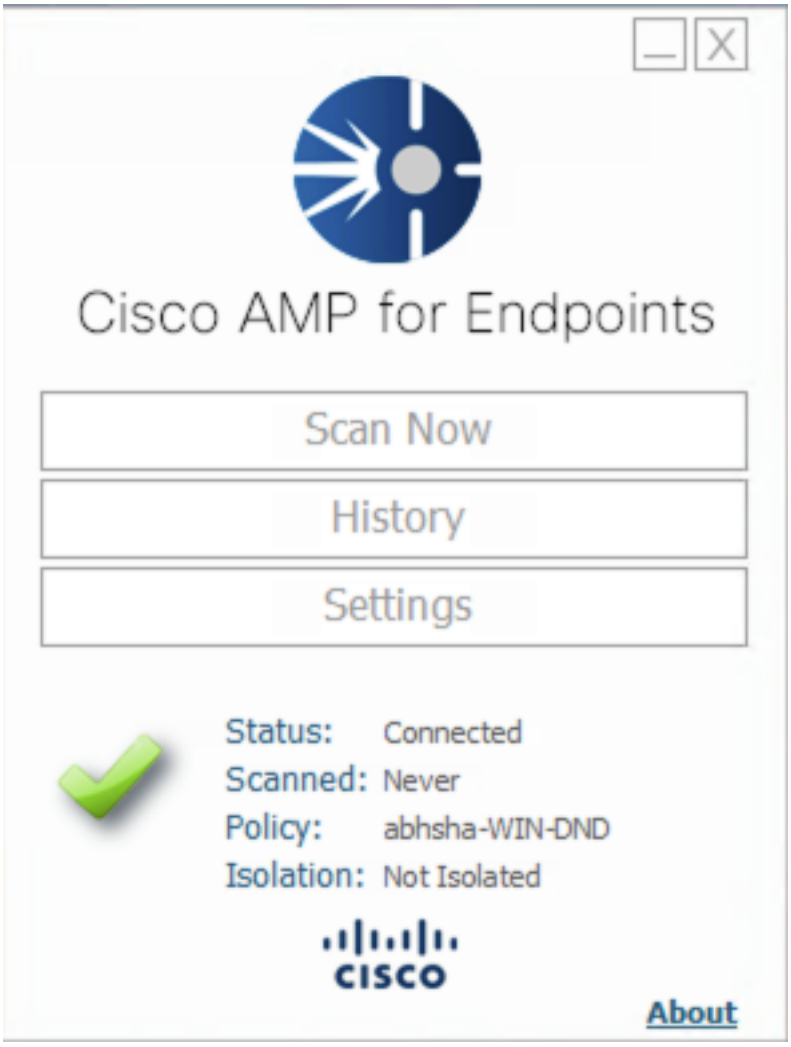
Inleiding

Dit document beschrijft de procedure om de Cisco Advanced Malware Protection (AMP)-connector te verwijderen als de installatie wordt geblokkeerd door de verbindingsbeveiligingsfunctie waarvoor een wachtwoord moet worden geleverd, en dat wachtwoord wordt vergeten. Er zijn 2 scenario's in dit geval, en dit hangt af van de vraag of de connector "Connected" met de AMP-cloud toont. Het is alleen van toepassing op Windows OS, omdat de connector Protection een functie is die alleen op Windows OS beschikbaar is.

Aansluiting is aangesloten

Stap 1. Klik op het pictogram en open de Cisco Advanced Malware Protection voor endpoints.

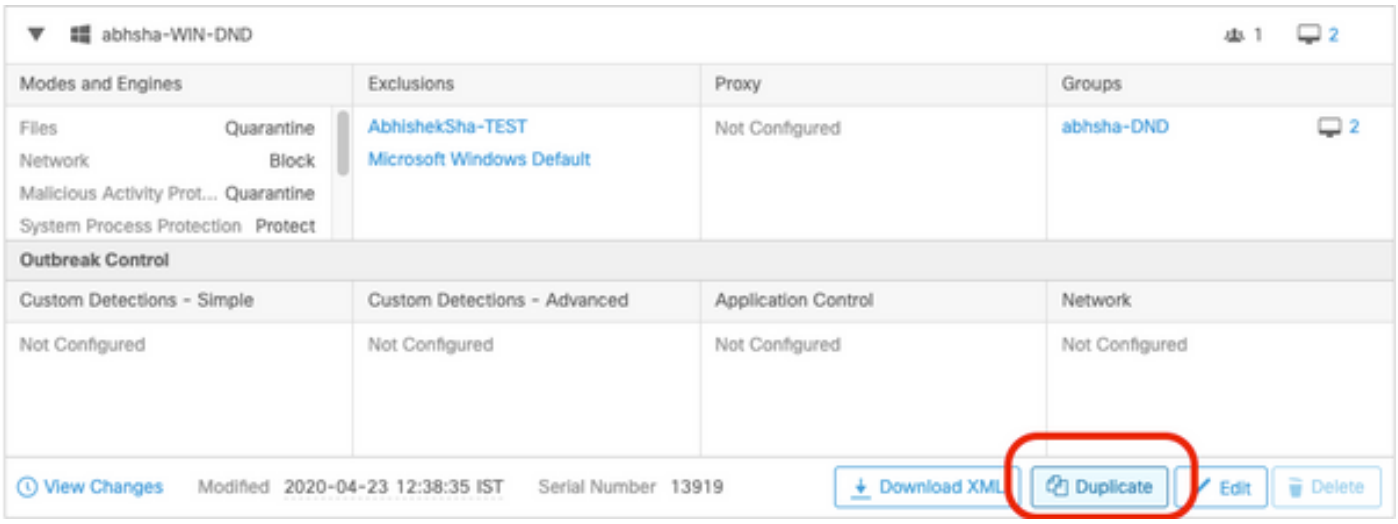
Stap 2. Zorg ervoor dat de connector is zoals aangesloten.



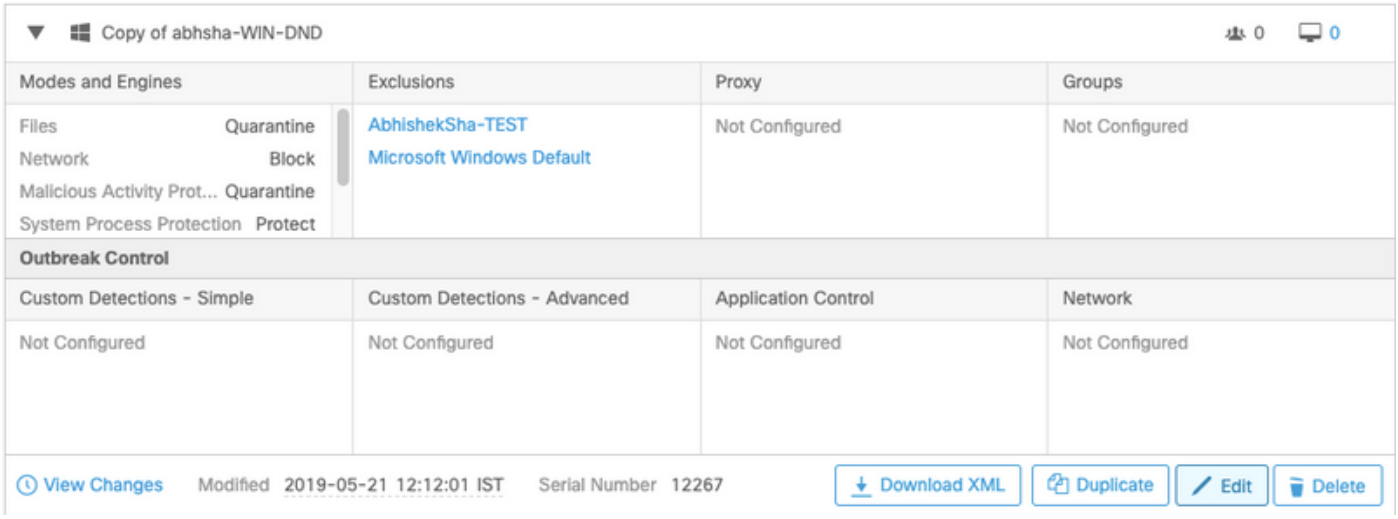
Stap 3. Let op dat het beleid aan die connector is toegewezen.

Stap 4. Navigeer naar uw Advanced Malware Protection voor endpoints en zoek naar het beleid dat eerder is opgemerkt.

Stap 5. Vul het beleid uit en klik op **Duplicaat** zoals in de afbeelding.

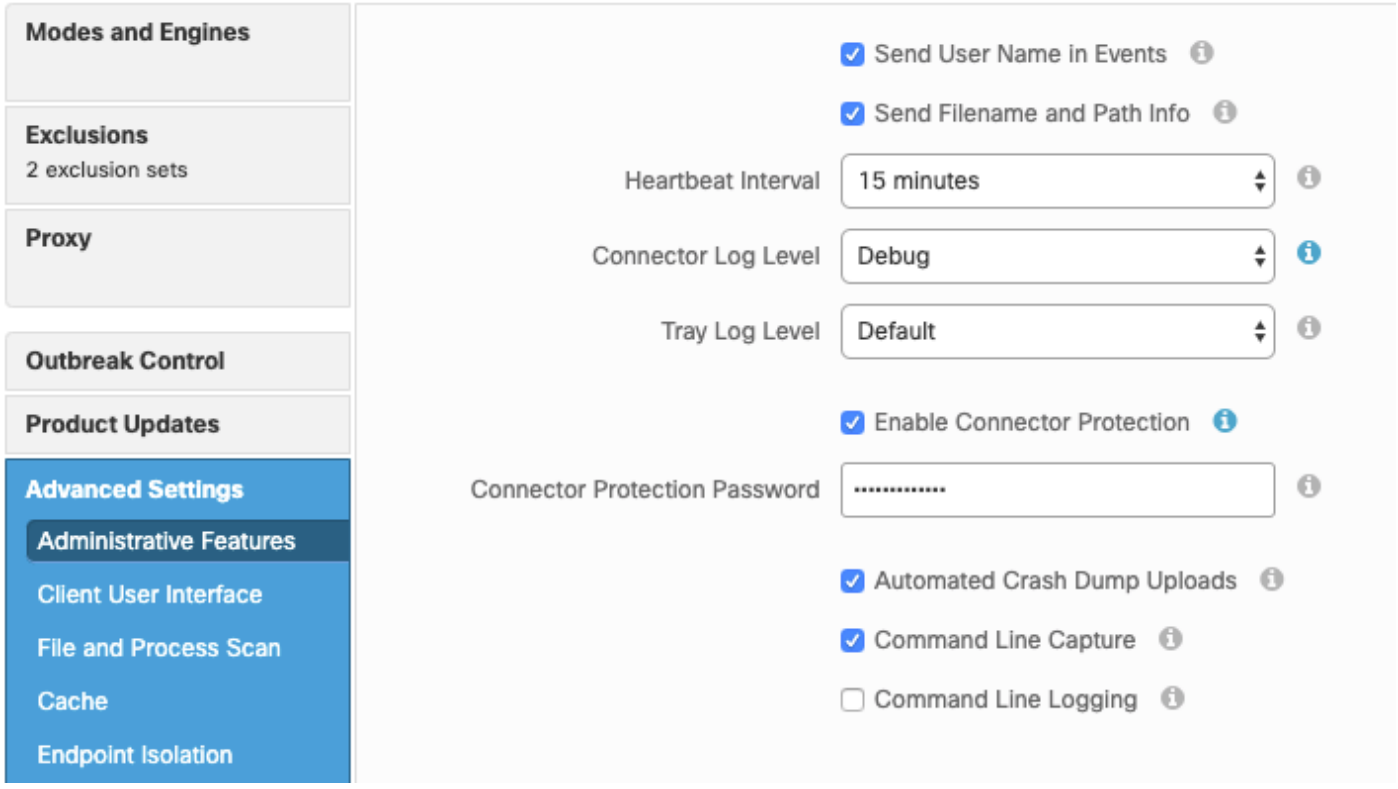


Stap 6. Een nieuw beleid genaamd "Kopie van.." wordt opgericht. Klik op **Bewerken** om dit beleid te bewerken zoals in de afbeelding.



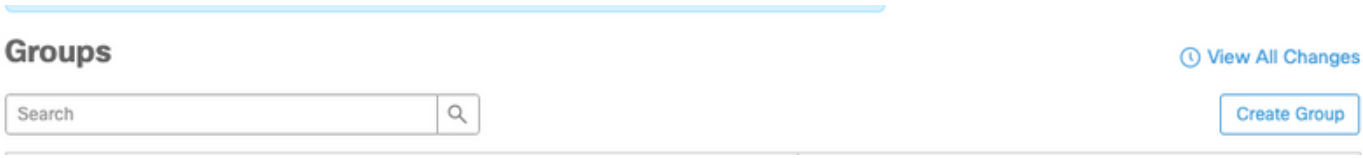
Stap 7. Klik op de pagina **Beleid bewerken** op **Geavanceerde instellingen > Administratieve functies.**

Stap 8. In het veld **Wachtwoord voor connectie** vervangt u het wachtwoord door een nieuw wachtwoord dat kan worden opgeroepen zoals in de afbeelding.

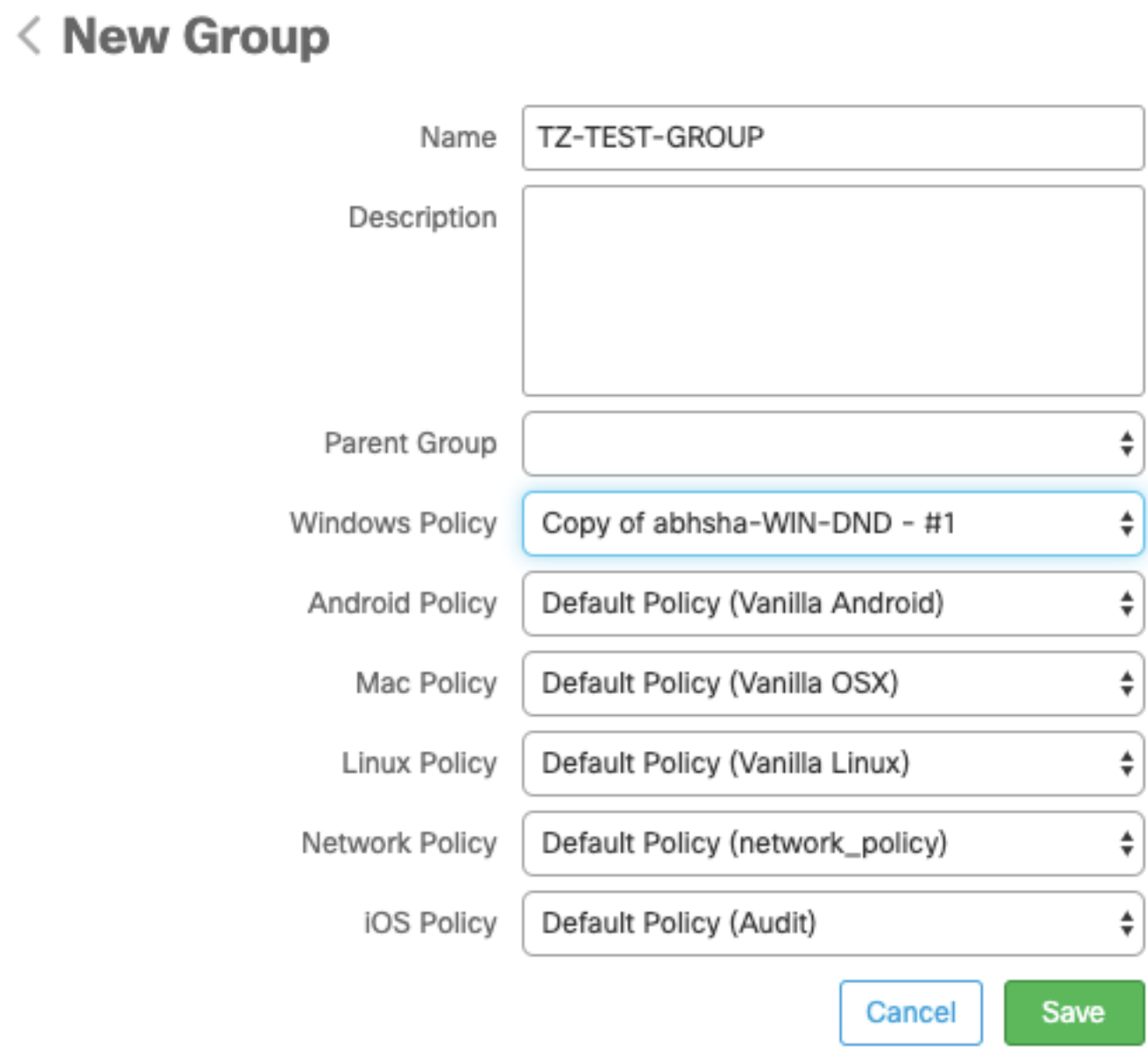


Stap 9. Klik op de knop **Opslaan** om dit beleid op te slaan.

Stap 10. Navigeer naar **Management > Groepen** en maak een nieuwe groep aan.

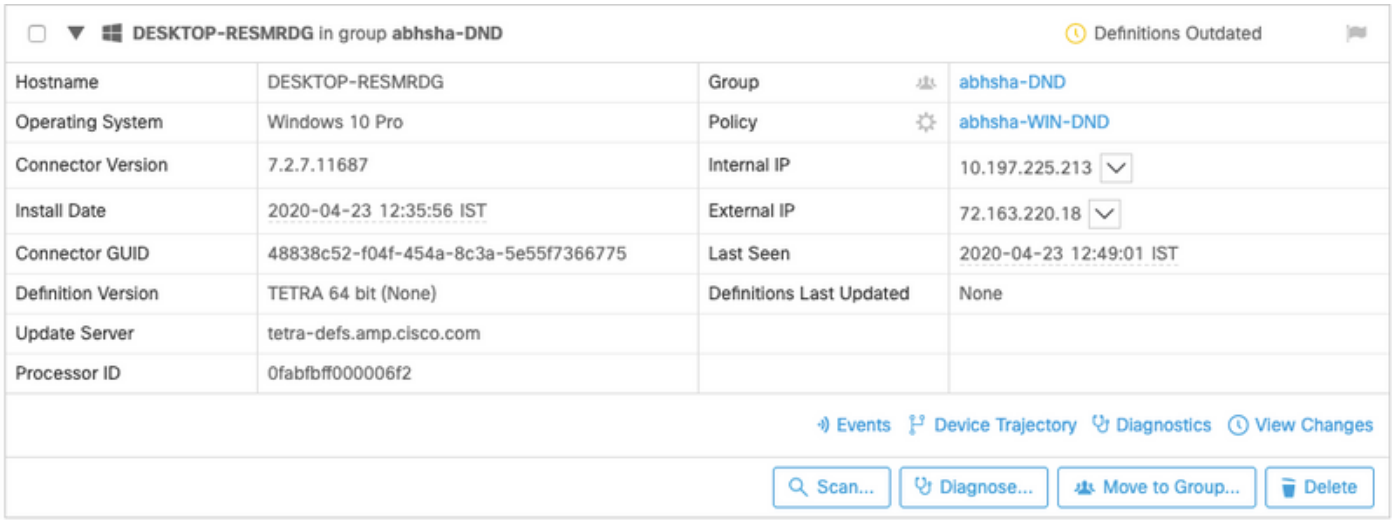


Stap 1. Voer een groepsnaam in en selecteer het **Windows-beleid** als het eerder bewerkte beleid. Klik op de knop **Opslaan** zoals in de afbeelding.



Stap 12. Navigeer naar **Management > Computers** en zoek naar de computer waarop u de AMP-connector wilt verwijderen.

Stap 13. Vul de computer uit en klik op **Verplaatsen naar groep**. Selecteer de laatst gemaakte groep in het dialoogvenster dat nu wordt weergegeven.



Stap 14. Wacht tot het beleid op het eindpunt wordt bijgewerkt. Het duurt gewoonlijk ongeveer 30 minuten tot 1 uur en is afhankelijk van het ingestelde interval.

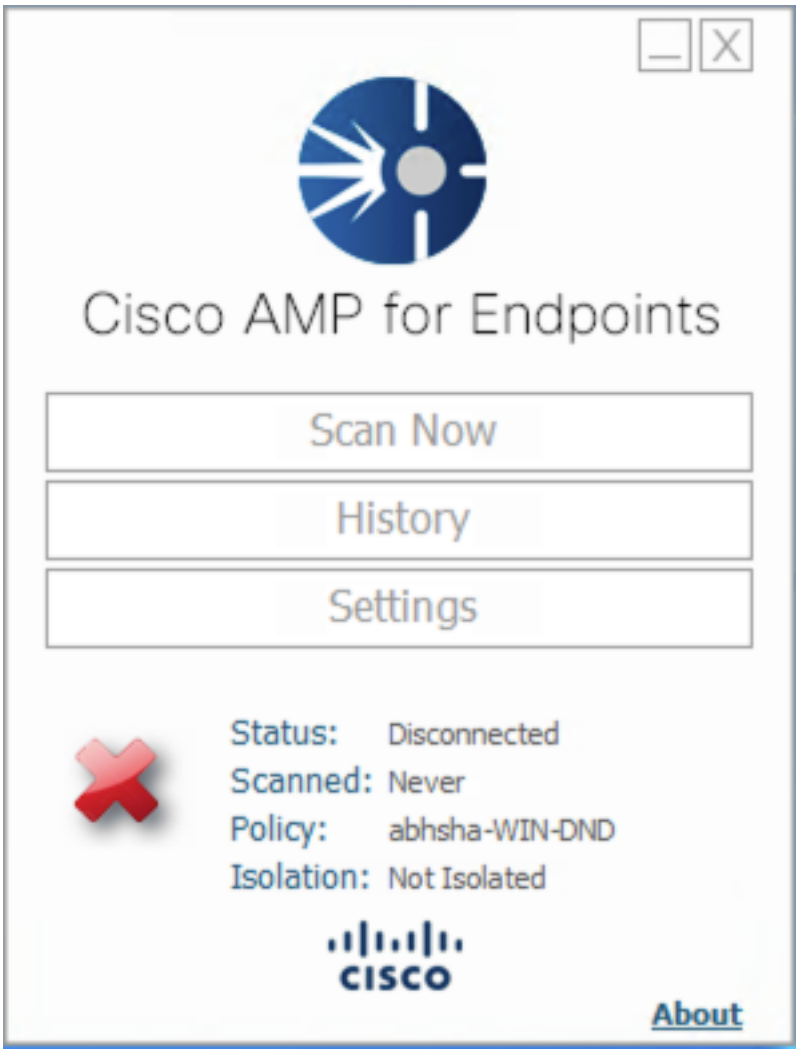
Stap 15. Zodra het beleid op het eindpunt is bijgewerkt, kunt u de connector verwijderen met het wachtwoord dat u onlangs hebt ingesteld.

Aansluiting is verbroken

Als de connector van de AMP-cloud is losgekoppeld, is het belangrijk om de computer in Safe Mode te kunnen starten.

Stap 1. Klik op het pictogram en open de Cisco Advanced Malware Protection voor endpoints.

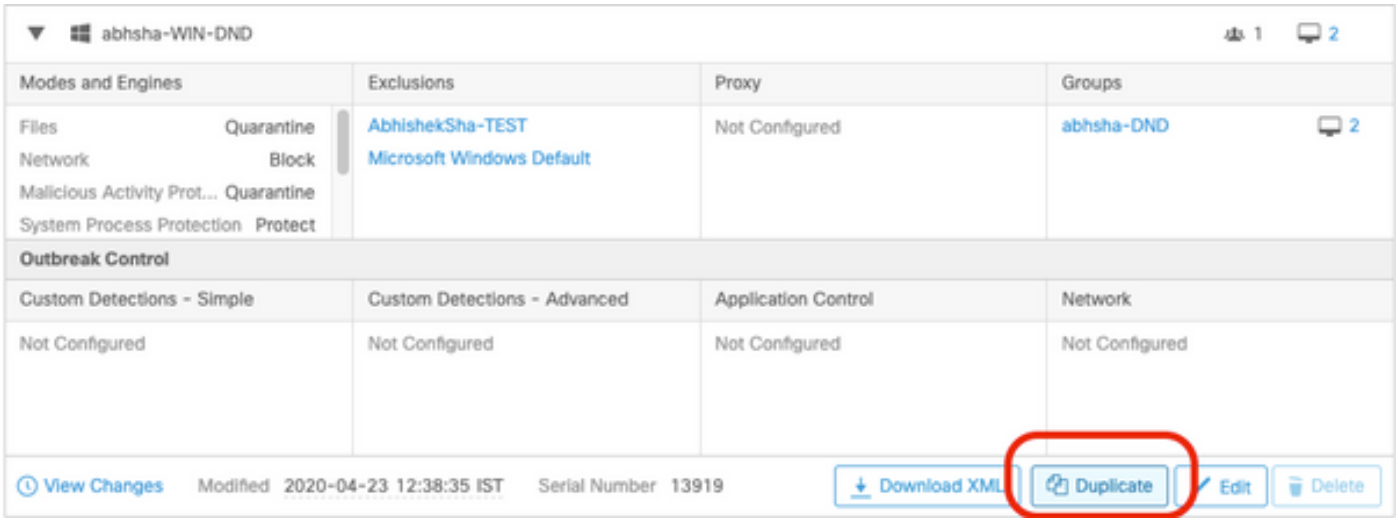
Stap 2. Zorg ervoor dat de connector als losgekoppeld is weergegeven.



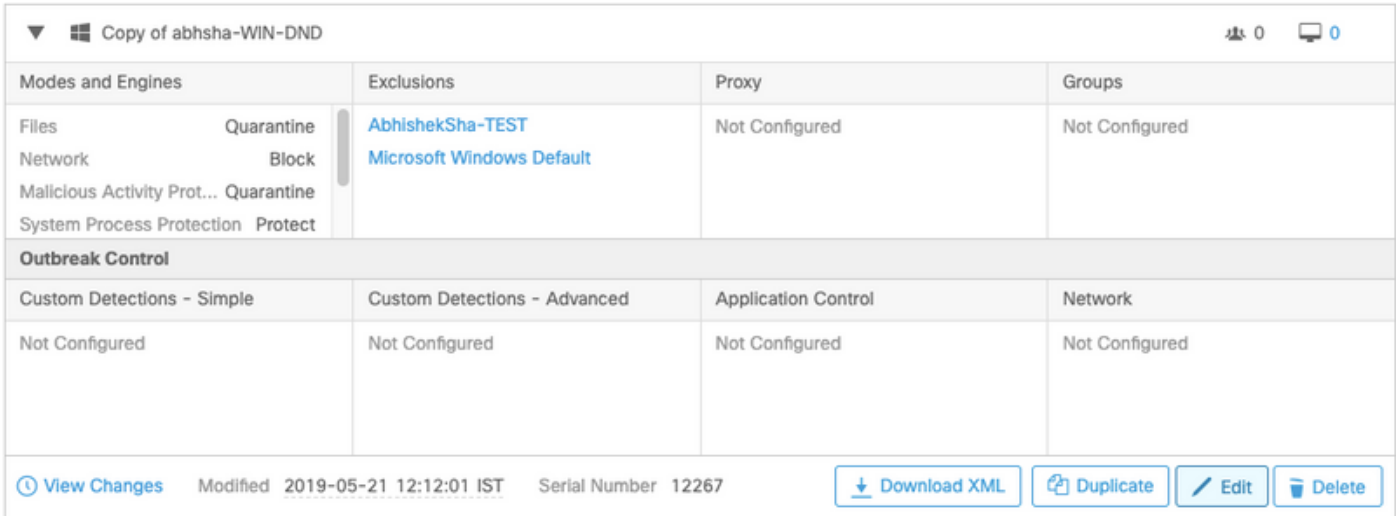
Stap 3. Let op het beleid dat aan die connector is toegewezen.

Stap 4. Navigeer naar uw Advanced Malware Protection voor endpoints en zoek naar het beleid dat eerder is opgemerkt.

Stap 5. Vul het beleid uit en klik op **Duplicaat** zoals in de afbeelding.

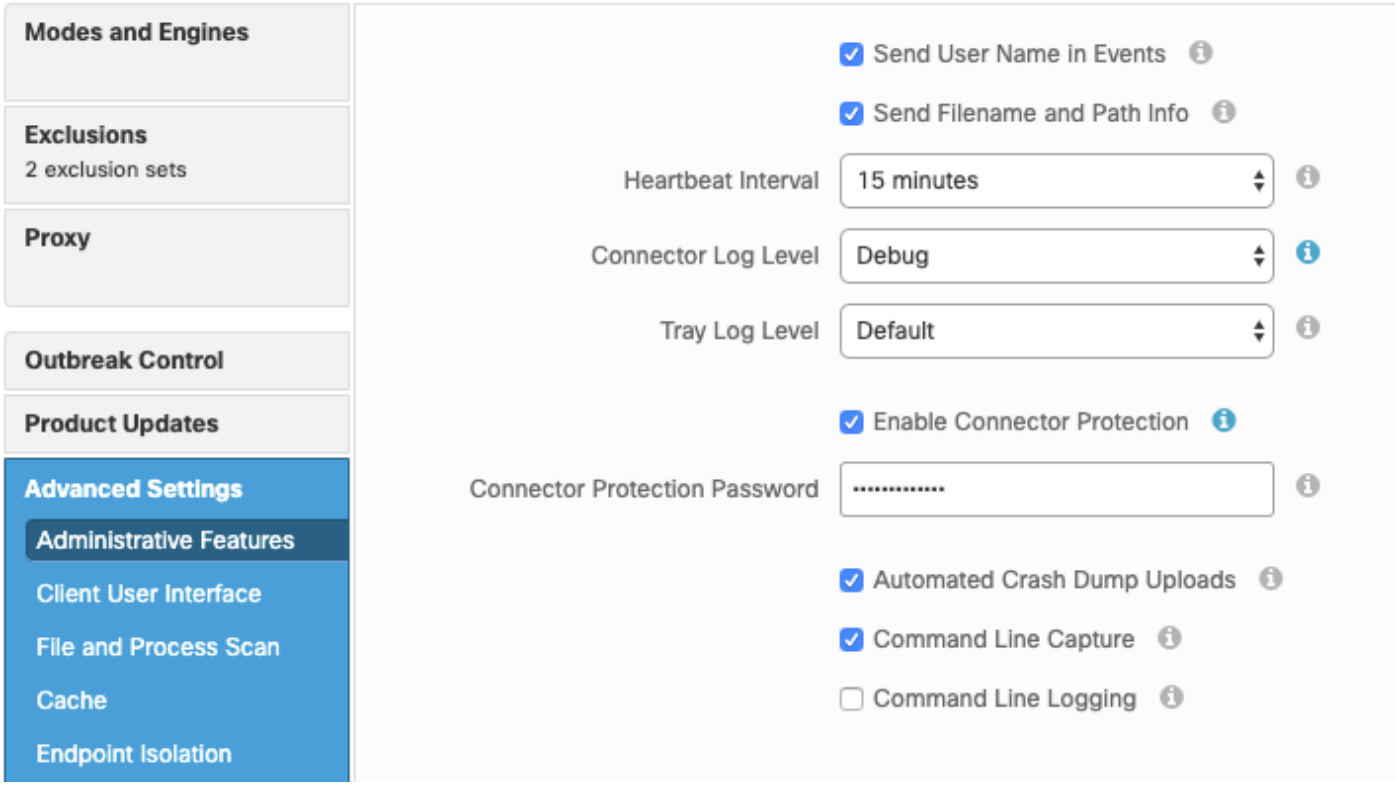


Stap 6. Een nieuw beleid genaamd "Kopie van.." wordt opgericht. Klik op **Bewerken** om dit beleid te bewerken.



Stap 7. Klik op de pagina Beleid bewerken op **Geavanceerde instellingen > Administratieve functies**.

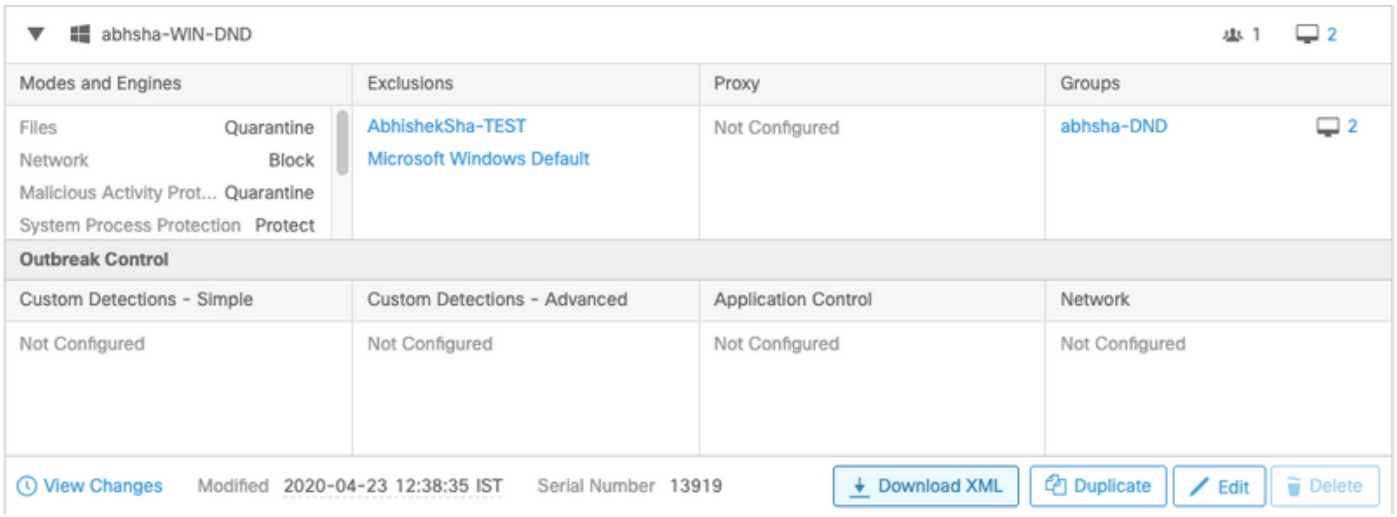
Stap 8. In het veld **Wachtwoord voor connectie** vervangt u het wachtwoord door een nieuw wachtwoord dat kan worden opgeroepen.



Stap 9. Klik op de knop **Opslaan** om dit beleid op te slaan.

Stap 10. Navigeer naar **Beheer > Beleid** en zoek naar het nieuwe beleid.

Stap 1. Vul het beleid uit en klik op **Download XML.** Een bestand met de naam **policy.xml** wordt op uw machine opgeslagen.

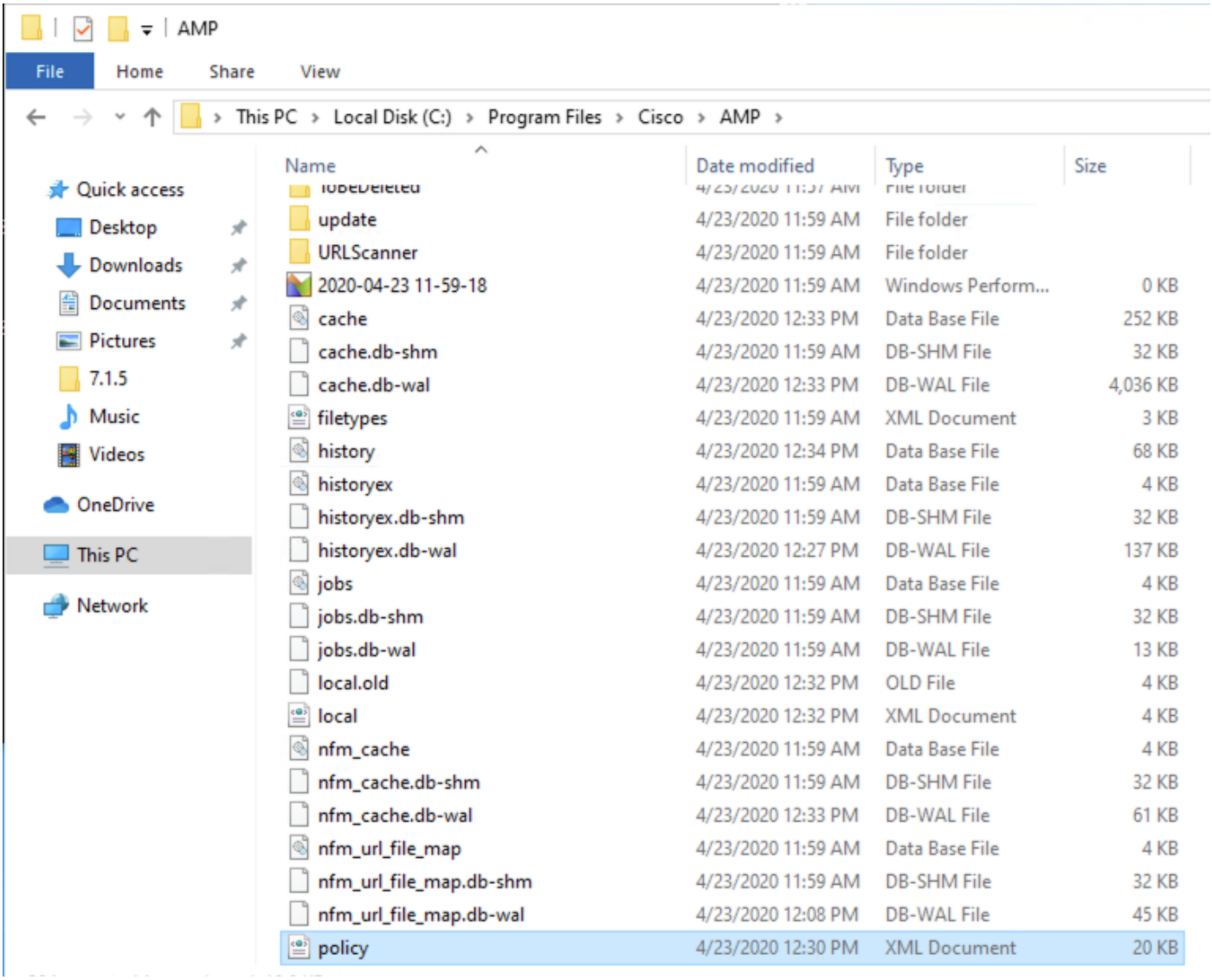


Stap 12. Kopieer dit **beleid.xml** naar het getroffen eindpunt.

Stap 13. Herstart het getroffen eindpunt in **Safe Mode**.

Stap 14. Nadat het getroffen eindpunt in **Safe Mode** is, navigeer dan naar **C:\Program Files\Cisco\AMP**.

Stap 15. In deze map selecteert u een bestand met de naam **policy.xml** en geeft u deze naam aan **policy_old.xml**.



Stap 16. Plaats nu het eerder gekopieerde **beleid.xml** in deze map.

Stap 17. Nadat het bestand is gekopieerd, kan de installatie normaal gesproken worden uitgevoerd en moet het wachtwoord worden ingevoerd.

Stap 18. Dit is een optionele stap. Aangezien de connector niet is geïnstalleerd toen de machine werd losgekoppeld, blijft de computeringang op de console. Daarom kunt u navigeren naar **Beheer > Computers** en het getroffen eindpunt uitbreiden. Klik op **Verwijderen** om het eindpunt te verwijderen.